



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/632,446

07/31/2003

Amit Raikar

200300489-1

2839

22879

7590

11/16/2007

HEWLETT PACKARD COMPANY

P O BOX 272400, 3404 E. HARMONY ROAD

INTELLECTUAL PROPERTY ADMINISTRATION

FORT COLLINS, CO 80527-2400

EXAMINER

SHIN, KYUNG H

ART UNIT

PAPER NUMBER

2143

MAIL DATE

DELIVERY MODE

11/16/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/632,446	<b>Applicant(s)</b> RAIKAR, AMIT	
	<b>Examiner</b> Kyung H. Shin	<b>Art Unit</b> 2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 August 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

1. This action is responding to application papers filed on **8-27-2007**.
2. Claims **1 - 19** are pending. Claim **1, 8, 14** are independent.

### ***Response to Arguments***

3. Applicant's arguments filed 8/27/2007 have been fully considered but they are not persuasive.

3.1 Replacement Figure 2 is accepted. (see Remarks Page 6)

3.2 Applicant argues that the referenced prior art does not disclose, "determining whether data associated with at least one message received by the template should or should be processed by the template". (see Remarks Page 8)

Based on the specification, a template (spec paragraph [0041]) is defined as, "The templates provide the interceptors with instructions on how to analyze and/or process the messages the interceptors receive." Interceptors intercept application and network management messages such as console, log file, and SNMP network management event messages. Desai discloses the processing of SNMP and log type messages. (see Desai paragraph [0043], lines 3-8; paragraph [0090], lines 4-10: SNMP, or logfile processing)

Desai discloses the usage of configured templates for determining whether a message should or should not be processed. (see Desai paragraph [0089], lines 7-9;

Art Unit: 2143

paragraph [0093], lines 1-3: configuration for analysis) Desai discloses a determination whether a message is acceptable (whether to process) or unacceptable (whether not to process). (see Desai paragraph [0056], lines 1-13: determination message false positive, message not processed further, abnormal) Some processing of the message must occur in order to determine whether to process the message any further.

3.3 Applicant argues, "filters cannot be relied on to teach certain features". (see Remarks Page 8)

The term Desai uses for a function cannot remove the fact that Desai discloses configuration of a template (a mechanism to analyze message). And, Desai discloses the processing and analysis of messages (template processing) using that configured template. (see Desai paragraph [0089], lines 7-9; paragraph [0093], lines 1-3: configuration; paragraph [0022], lines 1-5; paragraph [0101], lines 2-4: template processing) Desai disclose multiple steps (event analysis engine, event correlation engine, data threshold comparison and analysis) in the analysis of a message. (see Desai paragraph [0066]; paragraph [0075]; paragraph [0078]; paragraph [0062])

3.4 Applicant argues that the referenced prior art does not disclose, "configuring the template with third information for preventing the communication of at least one received message to other templates. (see Remarks Page 9)

In the event analysis engine, if a threshold is passed, then analysis takes a different path. Events are assigned a severity level and sent to central management server for further analysis and response. (see Desai paragraph [0098], lines 2-9;

paragraph [0099], lines 1-4: threshold analysis, alarm processing) If a threshold is not passed, then the message is further processed by event correlation engine. (see Desai paragraph [0078], lines 1-3: event correlation)

Applicant states that Desai templates are applied to data has been collected, parsed, normalized, and categorized. Additional features performed by the Desai reference do not remove the fact that Desai discloses the configuration of a template and the usage of a template to process messages. Claimed invention discloses the processing of a message by a template (processing instructions), which is used to analyze the message.

3.5 Applicant argues, dependent claims. (see Remarks Page 9)

Arguments for dependent claims are based upon above arguments for independent claims 1, 8, 14. The successful responses to arguments for independent claims 1, 8, 14, also respond to the current arguments against the dependent claims 2-7, 9-13, and 15-19.

3.6 Applicant argues, Flowers reference. (see Remarks Page 9)

Flowers reference is not used to remedy the limitations mentioned in remarks page 9. The Office Action states the limitations the Flowers reference is used to reject.

3.7 The examiner has considered the applicant's remarks concerning methods and systems for configuring secure templates for an application and network management system to provide network security. A template for an application and network

Art Unit: 2143

management system is configured with first information for determining whether at least one message received by the template should or should not be processed by the template. The template is configured with second information for processing data associated with at least one received message. The template is configured with third information for preventing the communication of at least one received message to other templates for the application and network management system. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Desai (20030188189) and Flowers (6,957,348) discloses the applicant's invention including disclosures in Remarks dated August 27, 2007.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1 - 7, 14 - 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Desai et al. (US PG PUB No. 20030188189).

**Regarding Claim 1**, Desai discloses a method for configuring templates, the method comprising:

- a) configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)
- b) configuring the template with second information for processing the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and
- c) configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

**Regarding Claims 2, 15**, Desai discloses the method, computer system of claims 1, 14, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server. (see Desai paragraph [0063], lines 1-4: forwarded to management server)

**Regarding Claims 3, 16**, Desai discloses the method, computer system of claims 1, 14, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template. (see Desai paragraph [0043], lines 3-8; paragraph [0090], lines 4-10: SNMP, or logfile processing)

**Regarding Claims 4, 17**, Desai discloses the method, computer system of claims 1, 14, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources. (see Desai paragraph [0050], lines 1-4; paragraph [0052], lines 1-6: matching utilized for analysis)

**Regarding Claims 5, 18**, Desai discloses the method, computer system of claims 1, 14, wherein the method further comprises: configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message. (see Desai paragraph [0058], lines 4-6; paragraph [0061], lines 7-11: event threshold parameter assigned to specific originating device)

**Regarding Claims 6, 19**, Desai discloses the method, computer system of claims 1, 14, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:



- a) configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked) and
- b) configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates. (see Desai paragraph [0063], lines 1-4: further analysis)

**Regarding Claim 7:** Desai discloses the method of claim 1, wherein the steps of configuring are performed by a template automator. (see Desai paragraph [0024], lines 1-3; paragraph [0062], lines 3-6; paragraph [0089], lines 5-9: automatic processing)

**Regarding Claim 14,** Desai discloses a computer system comprising:

- a) a memory unit; (see Desai paragraph [0012], lines 10-12: web server, network server, workstation) and
- b) a processor coupled to the memory unit (see Desai paragraph [0012], lines 10-12: web server, network server, workstation), wherein the processor executes instructions associated with a template automator, and wherein the instructions of the template automator are for:

- c) configuring a template for an application and network management system with first information for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)
- d) configuring the template with second information for processing the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and
- e) configuring the template with third information for preventing the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claim 8 - 13 are rejected under 35 U.S.C. 103(a) as being anticipated by **Desai et al.** (US PG PUB No. **20030188189**) in view of **Flowers et al.** (US Patent No. **6,957,348**).

**Regarding Claim 8;** Desai discloses a method for providing a guideline to developers for creating templates, the guideline comprising information used by the developers for:

- a) receiving first information entered by a developer to configure a template of an application and network management system for determining whether data associated with at least one message received by the template should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked)
- b) receiving second information entered by the developer to configure the template to process the data associated with at least one of the received messages; (see Desai paragraph [0093], lines 3-6: processing data, execute user defined programs) and
- c) receiving third information entered by the developer to configure the template to prevent the communication of at least one received message to other templates of the application and network management system. (see Desai paragraph [0063], lines 1-4: further analysis)

Desai does not specifically disclose the guidelines for developers. However, Flowers discloses wherein providing a guideline to developers for creating

templates, the guideline comprising information used by the developers. (see Flowers col. 2, lines 45-50; col. 2, lines 53-60: development of templates, rules)

It would have been obvious to one of ordinary skill in the art to modify Desai as taught by Flowers to enable the capability to provide a guideline comprising information used by the developers for creating templates. One of ordinary skill in the art would have been motivated to employ the teachings of Flowers in order to enable the capability to enable the identification and description of vulnerability and intrusion detection information for typical network engineers in development efforts. (see Flowers col. 2, lines 16-18: “ ... *Further, there is a need to perform vulnerability and intrusion identification and description that is usable by typical network engineers. ...* ”)

**Regarding Claim 9**, Desai discloses the method of claim 8, wherein configuring the template with second information for processing further comprises configuring the template with the second information for communicating the data associated with at least one of the received messages to a management server. (see Desai paragraph [0063], lines 1-4: forwarded to management server)

**Regarding Claim 10**, Desai discloses the method, of claim 8, wherein the template is one of an SNMP trap template, a message template, a monitor agent template, a logfile template and a console template. (see Desai paragraph [0043], lines 3-8; paragraph [0090], lines 4-10: SNMP, or logfile processing)

**Regarding Claim 11**, Desai discloses the method of claim 8, wherein at least one received message is validated with at least one of pattern matching language, MSI, values from environment variables, and values from secure sources. (see Desai paragraph [0050], lines 1-4; paragraph [0052], lines 1-6: matching utilized for analysis)

**Regarding Claim 12**, Desai discloses the method of claim 8, wherein the method further comprises: configuring the template with fourth information for specifying for a particular received message an action to be performed, wherein the fourth information ensures that the action is performed on a node that generated the particular received message. (see Desai paragraph [0058], lines 4-6; paragraph [0061], lines 7-11: event threshold parameter assigned to specific originating device)

**Regarding Claim 13**, Desai discloses the method of claim 8, wherein the second information specifies a superset of conditions for processing all the received messages and wherein:

- a) configuring the template with the first information further comprises configuring the template with the superset of conditions to determine whether data associated with at least one received message should or should not be processed by the template; (see Desai paragraph [0022], lines 1-5; paragraph [0023], lines 1-5: template processing; paragraph [0093], lines 3-6; paragraph [0094], lines 6-8: data is blocked) and

- b) configuring the template with the third information further comprises configuring the template with the superset of conditions to prevent the communication of at least one received message to other templates. (see Desai paragraph [0063], lines 1-4: further analysis)

### ***Conclusion***

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9:30 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KHS

Kyung H Shin  
Patent Examiner  
Art Unit 2143

KHS  
October 29, 2007



DAVID WILEY  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100